Appl. No. 09/895,692
Amdt. Dated: 01/10/2005
Reply to Office Action of 08/10/2004

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A state-varying hybrid stream cipher operating within a computing device, comprising:

a first software routine to divide incoming plain text into variable-sized blocks with each block varying in size; and

a second software routine to convert the plain text into cipher text based on an encryption key, an internal identifier and an internal state of the computing device.

2. (Original) The state-varying hybrid stream cipher of claim 1, wherein the first software routine produces the variable-sized blocks based on the encryption key, the internal identifier and an output of a first non-linear function.

3. (Original) The state-varying hybrid cipher of claim 2, wherein each current block of the plain text is determined by (i) producing a pseudo-random sequence using a second non-linear function including the encryption key, the internal identifier and the output of the first non-linear function as inputs and (ii) accessing contents of the pseudo-random sequence as a number of data elements of the plain text forming the current block.

4. (Original) The state-varying hybrid cipher of claim 1 further comprising:

a third software routine to determine if a plurality of random data elements are to be distributed within the cipher text and to compute a hash digest of the random data elements.

5. (Original) The state-varying hybrid cipher of claim 4 further comprising a fourth software routine to perform a first shuffling operation on the internal state of the computing device based on the encryption key so that a single bit modification of the encryption key

requires complete recalculation of the internal state of the computing device used to encrypt the random data elements.

6. (Original) The state-varying hybrid cipher of claim 4, wherein the second software routine further performs a second shuffling operation on the internal state of the computing device prior to encrypting the random data elements based on the encryption key and the internal identifier to mitigate a likelihood of prediction of the internal state of the computing device upon knowledge of the encryption key.

7. (Original) The state-varying hybrid cipher of claim 4, wherein the third software routine determines a statistical amount of random data elements distributed within the cipher text is programmable based on a percentage value entered by a user.

8. (Original) The state varying hybrid cipher of claim 7, wherein the distribution of random data elements within the cipher text is based on the encryption key, the internal identifier and internal state of the computing device.

9. (Original) The state-varying hybrid cipher of claim 1 further comprising a third software routine to distribute error correcting codes in the cipher text in order to correct modifications.

10. (Original) The state-varying hybrid cipher of claim 1, wherein the internal state of the computing device is periodically modified.

11. (Original) The state-varying hybrid cipher of claim 1, wherein the internal state of the computing device is based on a time value.

12. (Currently Amended) A computing device comprising:

a memory; and

logic coupled to the memory, the logic to perform a state-varying stream cipher operation, controlled by at least an encryption key and an internal state of the computing device, on input data segmented in random sized blocks using the encryption key.

13. (Original) The computing device of claim 12, wherein the stream cipher operation involves encryption.

14. (Original) The computing device of claim 12, wherein the logic is an integrated circuit.

15. (Original) The computing device of claim 12, wherein the internal state of the computing device varies over time.

16. (Original) The computing device of claim 15, wherein the variation of the internal state of the computing device is periodic being set at a time that an encryption process begins for each block of input data.

17. (Currently Amended) The computing device of claim 12, wherein the computing device is one of a smart card and an operating system.

18. (Currently Amended) The computing device of claim ~~15~~12, wherein the logic of the computing device ~~is an operating system~~ segmenting the input data into at least three random sized blocks with each block varying in length.

19. (Original) A method for decrypting input data using a combination of stream cipher and block cipher functionality, comprising:

receiving as input a cipher text, a decryption key, a percentage of random data and a unique internal identifier; and

reiteratively decrypting blocks of the cipher text using the decryption key, the percentage of random data, the unique internal identifier and a varying internal state of the computing device to recover corresponding blocks of plain text.

20. (Original) The method of claim 19, wherein the internal state of the computing device varies over continuously over time.